Chief Information Officer's Section
Office of the Governor
State of Utah

July 26, 2002

State Firewall Policy

Firewall Definition: For purposes of this policy, firewalls are defined as security systems, which control and restrict both Internet connectivity and Internet services. Firewalls either act as a protocol end point and relay (e.g., a SMTP client/server or a Web proxy agent), as a packet filter, or some combination of both (RFC 2979). Firewall functions establish a perimeter where access controls are enforced. Connectivity reflects which systems can exchange information. A service, sometimes called an application, refers to the way for information to flow through a firewall. Examples of services include file transfer protocol (FTP) and Web browsing (HTTP).

Firewalls in Practice: In some instances, systems of routers may be functioning as though they are firewalls when in fact they are not formally known as firewalls. All State of Utah systems functioning as firewalls, whether or not they are formally called firewalls, must be managed according to the rules defined in this policy. In some instances this will require that these systems be upgraded so that they support the minimum functionality defined in this policy. Any router that connects a vendor, other government, or any non-state entity, into the State network must employ *hardware and software standards approved by the ITPSC (Information Technology Policy & Standards Committee).* The introduction of a firewall and any associated tunneling or access negotiation facilities MUST NOT cause unintended failures of legitimate and standards-compliant usage that would work were the firewall not present (RFC 2979).

Policy Applicability: All firewalls at The State of Utah must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the Division of Information Technology Services (ITS).

Defined Decision Maker: Prior to the deploying of State of Utah firewalls, a list of permissible paths with the justification for each firewall must be submitted to ITS. Agency change control will be used to document any changes. Every network connectivity path not specifically permitted must be denied by firewalls.
Permission to enable paths will be granted by the agency security manager only when (1) the paths are necessary for business reasons, and, (2) adequate security measures will be used. State computer /data resources that exist on the authorized network must be secured from unauthorized traffic with the exception of production services designed to be homed in a "demilitarized" environment (http, internet mail), or where stateful packet inspection is not required. At a minimum, traffic filter firewall should have the ability to screen and log traffic at the network and transport protocol layers.

Default To Denial: Every Internet connectivity path and Internet service not specifically permitted by this policy must be blocked by State of Utah firewalls. The list of currently approved services must be documented and distributed to all systems administrators with a need-to-know by ITS.

Regular Auditing: Because firewalls provide the first barrier to unauthorized access to State of Utah networks, they must be audited on a regular basis. At a minimum, this audit process must include consideration of defined configuration parameters, enabled services, permitted connectivity, current administrative practices, and adequacy of the deployed security measures. These audits must also include the regular execution of vulnerability identification software. These audits must be performed by technically proficient persons other than those responsible for the administration of firewalls. The CIO, in consultation with SISC (State Information Security Committee) defines auditing procedures and responsibilities.

Logs: All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged. In addition, system activity (syslog), which might be an indication of, unauthorized usage or an attempt to compromise security measures must also be logged. The integrity of these logs must be protected with checksums, digital signatures, or similar measures. These logs must be promptly removed (what periodicity?) from the recording systems and stored in a physically protected container for at least three months. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

Intrusion Detection: State of Utah locations housing systems with sensitive, critical or access-restricted data must include intrusion detection systems approved by ITS or the agency consistent with the State Intrusion Detection Standard. Intrusion detection systems must be configured according to the specifications defined by ITS in cooperation with agencies. Intrusion detection systems must also immediately notify technical staff that is in a position to take corrective action when a problem occurs. All technical staff working on firewalls must be provided with remote access systems and privileges so that they can immediately respond to these incidents even when they are physically or logically removed from the firewall in question.

Contingency Planning: Technical staff working on firewalls must prepare and obtain ITS concurrence for contingency plans which address the actions to be taken in the event of various problems including system compromise, system malfunction, and power outage. These contingency plans must be kept up-to-date to reflect changes in the State of Utah computing environment. These plans must also be periodically tested to ensure that they will be effective in restoring a secure and reliable computing environment.

External Connections: All in-bound real-time Internet connections to The State of Utah internal networks and/or multi-user computer systems must pass through a firewall before users can authenticate. Aside from personal computers, which access the Internet on a single-user session-by-session basis, no State of Utah computer system may be attached to the Internet unless it is protected by a firewall. Such computer systems include web servers, electronic commerce servers, and mail servers.

Extended User Authentication: Inbound traffic (with the exception of Internet mail and push broadcasts) accessing State of Utah networks through a firewall must in all instances involve extended user authentication measures approved by ITS. Extended user authentication involves a technology more secure than fixed passwords and user-IDs. Examples of approved extended user authentication systems include Remote Authentication User Dial-In Service (RADIUS); Web single-sign-on (SSO) environments, and digital certificates.

Virtual Private Networks: To prevent unauthorized disclosure of sensitive and valuable information, connections to State resources (with the exception of Internet mail and push broadcasts) making access to State of Utah networks must be encrypted with the products approved as part of the Utah Technical Architecture. These connections are often called virtual private networks or VPNs, and include technologies such as Secure Sockets Layer (SSL), Secure Shell (SSH), IPSec, or other acceptable forms of encryption.

Firewall Access Privileges: Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a few individuals with a business need for these privileges, such as ITS Network Operations Center (NOC) personnel. Unless permission from the agency security manager has been obtained, these privileges will be granted only to individuals who are full-time permanent employees of the State of Utah (no temporaries, contractors, consultants, or outsourcing personnel). Vendor access for troubleshooting and technical support may be granted on an as needed basis. All firewalls must have at least two staff members who are adequately trained to make changes, as circumstances require or the NOC will be retained to make changes.

Secured Subnets: Portions of The State of Utah's internal network that contain sensitive or valuable information and must employ a secured subnet implementing non-routable or private IP network addressing. Access to this and other subnets must be restricted with firewalls and other control measures. Based on periodic risk assessments, ITS and agency security personnel will define the secured subnets required.

Network Management Systems: Firewalls must be configured so that they are visible to internal network management systems. Firewalls must also be configured so that they permit the use of remote automatic auditing tools to be used by authorized State of Utah staff members. Cisco Policy Manager and Cisco Works are the primary auditing and monitoring tools employed by ITS.

Disclosure Of Internal Network Information: The internal system addresses, configurations, and related system design information for State of Utah networked computer systems must be restricted such that neither systems nor users outside the State of Utah's internal network can access this information. Firewalls must be configured so they will not broadcast routes or Simple Network Management Protocol (SNMP) information on an outbound basis.

Secure Back-Up: Current off-line back-up copies of firewall configuration files, connectivity permission files, firewall systems administration procedural documentation files, and related files must be kept close to the firewall at all times. A permissible alternative to off-line copies involves on-line encrypted versions of these files. Either of these options will help to keep a trusted copies away from intruders, but at the same time immediately available to reestablish a secure and reliable computing environment. The NOC will be responsible for maintaining backup information on all router and firewall configurations.

Firewall Change Control: Because they support critical State of Utah information systems activities, firewalls are considered to be production systems. This means that all changes, including configuration changes as well as software upgrades and patches must be submitted with the plan of implementation to be approved in advance by ITS, and then tested and approved before being used in a production environment.

Any modification to the Internet firewall rule set exposes the State WAN to additional risk. Accordingly, any modification request will be subject to the approval of tier 5 Security personnel. Changes must be requested 10 days in advance of the needed change or include appropriate justification for expediency.

The requestor must provide documentation justifying the change and assume responsibility for ensuring that adequate security measures are in place on the internal (destination) resources, All openings in the firewall must be documented including requestor, date, purpose (business need), implementer, and responsible party(ies)..

Posting Updates: Because hackers and other intruders use the latest attack techniques, State of Utah firewalls must be running current (non-beta) software to repel these attacks. Where available from the vendor, all State of Utah firewalls must subscribe to software maintenance and software update services. Unless approved in advance by the agency security manager, staff members responsible for managing firewalls must install and run these updates within a a reasonable period following announcement of availability. This update provision may be met by local agency security personnel or the update may be requested from ITS.

Monitoring Vulnerabilities: State of Utah staff members responsible for managing firewalls should subscribe to CERT (Computer Emergency Response Team) advisories and other relevant sources providing current information about firewall vulnerabilities. Any vulnerability, which appears to affect State of Utah networks and systems, must promptly be brought to the attention of agency security managers and SISC.

Standard Products: Unless advance written approval is obtained from the State Technical Architect, only those firewalls referenced in the state Firewall Standard may be deployed with State of Utah networks. This standard is periodically updated.

Firewall Physical Security: The State must employ due diligence in ensuring physical security at any location where firewalls will be installed.

References:

Interim Date: July 26, 2002
Organization Sponsoring the Standard: ITS, State Information Security Committee (SISC)
State Technical Architect Approval Date: Pending
CIO Approval Date: Pending
ITPSC Presentation Date: 6/27/02 for comment, 8/1/02 for approval
Author(s): Robert Woolley, John Malouf, Rick Gee (ITS)
Related Documents: State Firewall Policy, Intrusion Systems Detection Standard, and Virtual Private Network (VPN) Standard, State Information Security Policy, State Network Access Policy